

Method and Apparatus for Secure Transmission of Data and Applications

Abstract

- 5 Authenticated transmissions are usually time-consuming and often provide
delayed error recognition and correction. This is a problem particularly with
hand-held computing devices like personal digital assistants (PDAs), smart phones
or smartcards, since these usually possess limited memory, processing power and
communications bandwidth. Because of these limitations and generally low trans-
10 fer rates between the device and a provider or central computer base, such trans-
missions are time-consuming and delay applications. The late detection of
unavoidable transmission errors is especially cumbersome. By applying an opti-
mally tailored authentication scheme to a block-wise transmission and in particu-
lar by applying a tree structure for the authentication process during such transfers,
15 the present invention minimizes the unavoidable delays and thus provides a solution
for these problems.